Chapter 35 - Locks and Keys

3501 Security Requirements

The Department of Commerce aims to provide safe and secure workplaces that are open and inviting for all departmental employees and visitors, yet maintain accountability of keys, safes, and vaults. Requirements for selection of locks to provide security for the respective working environments will depend on the assets to be protected and the local conditions. The security of any property or facility relies heavily upon locking devices. Locks merely delay entry and should be supplemented with other protective devices. An assessment of all hardware, including doorframes and jambs, should be included in any physical security survey. Devices, which vary greatly in appearance as well as function and application, are described below in paragraph 3502, Types of Devices.

3502 Types of Devices

A. Key Locks. Key locks are the most common locks. They include mortise cylinders, rim cylinders, padlocks, cylindrical lock-sets, and tubular lock-sets. Although a determined individual can open most key locks in a few minutes, locks are used primarily to delay and discourage or deter theft or unauthorized access.

B. Computerized Combination Locks. New technology now uses computerized dialers and robotics to unlock mechanical combination locks. Facility managers or security contacts should refer to the GSA schedule for approved computerized combination locks and specifications.

C. Mechanical Manipulation-Resistant Combination Locks. Manipulation-resistant combination locks are no longer available through the GSA procurement system as approved combination locks. They still provide a high degree of protection and those already in service may be used to protect classified material. Locks requiring major repairs must be replaced with a computerized combination lock meeting Federal Specification FF-L-2740. Minor repairs to the lock do not affect the storage approval of the container. Some of the more commonly used locks include the following.

1. Sargent and Greenleaf (S&G) 8400 MP locks are built-in three wheel combination locks. These locks can be installed on safes, security containers, vaults, and doors protecting secured areas.

2. The Mosler 302 Lock is a built-in, three-wheel combination lock, and can be installed on safes, security containers, and vaults, but not on doors. Locks presently in service may remain in service until major repairs are required.

D. Combination Padlock. The combination padlock is used primarily on the bar-lock filing cabinets. They are approved for storage of classified material up to and including Secret until October 1, 2012. Types of padlocks currently approved for use at Departmental facilities include the following locks.

1. S&G Model 8077 is enclosed in a chromed metal shell protecting the body of the padlock. The change key hole is located in the back of the padlock. The stated protection afforded by the exposed shackle Model 8077 is 30 man-minutes against manipulation of the lock, 30 man-minutes against radiological attack, and 10 man-minutes against surreptitious entry.

2. S&G Model 8077AB is an updated version of the Model 8077. There is no protection rating available for this lock.

E. Electro-Mechanical Cipher Locks. Electro-mechanical cipher locks are primarily used to control entry into an area. Rather than using a key, a person opens a lock by pushing a series of numbered buttons. The lock can be activated either electrically or mechanically. Examples include the Simplex Lock (mechanical) and the Continental Model S (electric). Two of the advantages of using these locks are easy combination changing and simple operation. These devices are used for access control and do not provide a high degree of security when used alone. Some models have "time penalty" and error alarm features and can be tied to an existing alarm system. When used in a controlled or restricted area that is not manned 24-hours, these locks must be supplemented by a built-in combination lock described above.

F. Electronic Card Key Systems.

1. An electronic access control system uses a card key programmed with a particular code which is read by a card reader that communicates with an automated central processor. The card reader obtains data from the card by reading punched holes, magnetic strips or spots, imbedded wires, or any of several other methods. To open a door, the card is typically inserted into a slot, swiped through a groove, or placed in proximity to a sensor, and the coded area is read by the system's reader. If the code is an authorized one, the processor will direct the lock to open.

2. Card readers fall into two basic categories: on-line and intelligent.

a. On-line readers must communicate with a central processor that makes the entry/exit decision.

b. The intelligent card reader compares the data on the card with preprogrammed data and entry or exit is granted or denied by the card reader itself at the reader location. Intelligent readers are also called stand-alone or off-line readers.

3. Multiple card readers can be used to control access to numerous buildings and rooms on one central processor. Most processors are capable of discriminating between time zones and levels of status for multiple readers and recording the time, date, location, and frequency of employee movements in and out of an area. Many have additional features and capabilities such as monitoring alarms, keeping time and attendance records, and communicating with emergency and law enforcement agencies.

G. Biometric Systems. Other locking systems are available which use neither keys nor combinations. These systems include locks that open by identifying a fingerprint, voiceprint, or retinal image. These biometric systems are primarily designed to control access to extremely sensitive, special-use areas where positive personal identification is an operational necessity. Facility managers or security contacts should consult with local security professionals or contact the Office of Security for further guidance on technical specifications.

3503 Changing A Combination

A. When to Change a Combination. The combination to a lock should be changed when:

1. The container or lock is received or put into service;

2. Any person having knowledge of the combination leaves the organization;

3. There is reason to believe it has been compromised; or

4. The container is taken out of service.

B. Selecting a Combination. When selecting combination numbers avoid multiples of five, ascending or descending numbers, simple arithmetical series, and personal data such as birth dates and Social Security numbers. Use numbers that are widely separated. This can be achieved by dividing the dial into three parts and using a number from each third as one of the combination numbers. Numbers should be in high-low-high or low-high-low sequence. The same combination

should not be used for more than one container in the same office. Carefully follow any manufacturer's instructions in installing combination numbers.

C. How to Change a Combination. Combination locks have either hand-change or key-change capability.

1. **Hand-Change Lock.** To change the combination in a hand-change lock, remove the disks from the lock one at a time, and keep them carefully in order. Change each disk from the old to the new combination and replace them in the order in which they were removed.

2. **Key-Change Lock.** To change the combination of a key-change lock, refer to the manufacturer's instructions. Be sure to insert the proper change key into the lock case. A different key may not release all disks. To prevent a lockout, try a new combination at least three times before closing the shackle or container.

D. Safeguarding the Combination.

1. Only those persons whose official duties require access to a security container should know its combination. The written combination should be protected at the highest classification level of material in the container. The combination should be sealed in an envelope and kept by the servicing security officer. The SF-700, Security Container Information, will be used for this purpose. Instructions appear on the form.

2. Combinations should be memorized. They must not be carried in wallets or concealed on persons, or written anywhere other than the SF-700. The SF-700 form will be stored in a security container rated for the highest level of classification of the material to be protected.

3. When opening any kind of combination lock, personnel must ensure that no unauthorized person can learn the combination by observing the sequence of numbers being entered or dialed. It may be necessary to block the view of the dial from anyone standing nearby.

3504 Keys

A. Types of Keys.

1. **Operating or Change Keys.** Keys that employees use daily to open locks.

2. **Duplicate Keys.** Copies of change keys that are usually stored for use in an emergency or to replace a lost key. Duplicate keys must be kept to a minimum and be protected to avoid proliferation and loss of accountability.

3. **Master Keys.** Keys designed to open all locks of a particular series. Key systems can have one grand-master key for the overall system and several sub-master keys for each subsystem. Master keys can be used as a convenience, but must be carefully controlled.

4. **Construction Keys.** Keys that open the locks installed on the doors during the construction of a facility.

5. **Control Keys.** Keys used to remove the cores of locks for changing keys. These keys are used only in interchangeable core systems.

6. **Restricted Keys.** Key blanks controlled by the manufacturer and provided only to authorized issuing officials.

B. Accountability Procedures.

1. The integrity of a key system is important to safeguard property and control access to restricted areas. Lost keys minimize the effectiveness of a lock. The facility manager or servicing security officer must provide specific guidance for maintaining the facility's key system to include storing, issuing, and accounting for all keys of a system. Keys should be issued only to persons who have an official need. Keys not issued should be stored in a locked container.

2. The loss of a key must be reported immediately to the issuing office, preferably by telephone, followed by a written report within three working days with a copy forwarded to the servicing security officer. The report must include a detailed explanation of the circumstances surrounding the loss. Accountability records must be kept accurately, and the issuing official should follow the instructions noted below.

a. When a key to a designated controlled or restricted area is lost, the locks to the area must be changed.

b. Access lists for persons authorized to draw master keys shall be maintained.

c. The key storage container shall be checked at least monthly.

d. All keys shall be inventoried at least annually.

3. Requests for issuance of new, duplicate, or replacement keys shall be approved or monitored by the facility manager or the servicing security officer.

4. Systems used to account for keys must include the following information:

a. Inventory number assigned to each key and lock;

b. Location of each lock (room number);

c. Name of person to whom keys have been issued;

d. Date of issuance;

e. Room numbers that the key will open; and

f. Signature of the recipient to whom the keys are issued.

C. Protection of Keys.

1.Personnel must never put an identifying tag on their office key ring. If lost, it is an open invitation to thieves.

2. Office keys should be kept on one ring and personal keys on another. Personal keys should not be tagged or identified since this can lead thieves directly to your house or car.

3. Office keys should not be left on a desk, under a typewriter, or in an unlocked drawer where they can be easily taken and copied. Office, car, or house keys should not be placed in a coat and left hanging on a coat rack or draped over a chair. Office and personal keys should be kept with a person or locked securely in a desk or cabinet.

4. An office key should not be lent to anyone.

5. If office keys are missing, personnel should immediately report the incident to the issuing officer or a member of the guard force. A security evaluation should be conducted to determine the need to re-key the office.

6. Security contacts, facility managers, or other issuing officials should institute a waiting period of 10 work days for the replacement of lost keys. The waiting period will allow time for the lost key to be found before expending the time and expense of issuing a replacement key. Offices that issue keys should establish alternative procedures for entry by employees during the waiting period.